Data collection sources, techniques and analytical processes: What's the Big Data deal?

Big Data has become quickly evolved into an usually powerful resource that has the capability to provide insights that were previously elusive or unattainable.

Greg Gogolin, Ph.D., CISSP, PMP
Ferris State University
Challenge #1

Legal aspects, ethical use and social norms are often an afterthought.
Challenge #2

- Humans

- Organizations seek to enrich themselves

- Nations seek advantage
Challenge #3

Big Data itself

- Active and Passive data gathering
- Internet of Things (IoT)
- “Smart” devices
- Apps
- Privacy Policies
Challenge #4

Lack of understanding

- Apathy
- Scope
- Threat Identification
- Ignorance that a problem exists

“I wish I didn’t know now what I didn’t know then.” – Bob Seger
Scenario 1: Information Disclosures & Security Vulnerabilities of IoT Devices.

Smart TV & Amazon Echo

Greg Gogolin, Ph.D.
Professor
Information Security & Intelligence

James Furstenberg, M.S.
Assistant Professor
Information Security & Intelligence

Kaushik Bindu Sai. Yelisetti
Graduate Research Assistant

Madhurima. Vadlamudi
Graduate Research Assistant
Madhurima Vadlamudi & Kaushik Bindu Sai Yelisetti
Introduction/Background

• “... by the year 2020 there will be over 50 billion internet-connected smart devices”

• “IoT devices capture and relay end user information to manufacturers and other parties without the knowledge or consent of the end user”

• “... user privacy is a very important challenge of IoT”

• By 2020, over 25% of identified attacks in enterprises will involve IoT, though IoT will account for less than 10% of IT security budgets.

(Vergetis Lundin, 2015)
Research Objectives

• Information Disclosure
  – Active and Passive - voice capturing and monitoring abilities of voice active commands.
  – Verboseness of Data sent over the network
    • including what was sent and where it was sent.
  – Confidentiality of communication transmissions over the network.
  – Activity state testing
    • i.e. standby state, voice command and how often the device checked into the network.
• Testing for voice log data and traffic from the apps used to
Device 1 - Amazo

• Deceptively Simple
• Very popular personal automated assistant.
• Seemingly innate and harmless.
• Voice automated operation.
• Integrated with mobile phone Alexa App.
Echo Setup

Begin Echo setup

Let's get your Echo connected to Wi-Fi so you can start using it.

Connect to Wi-Fi

Cancel setup

Echo Setup

Wait for the orange light ring

Make sure your Echo is plugged into a power outlet. In about a minute, the light ring will turn orange. Then continue.

Continue

Cancel setup

Don't see the orange light ring?

Wireless Search

Connect your iPhone to Echo

Go to your Wi-Fi settings on this iPhone and select the network of the format Amazon-XXX. It may take up to a minute to display. Wait until Echo says you are connected, then return to this screen.

Cancel setup

Don't see the orange light ring?

Setup Complete
Echo Motherboard

Deceptively Powerful

- Texas Instruments DM3725CUS100 Digital Media Processor
- Samsung K4X2G323PD-8GD8 256 MB LPDDR1 RAM
- SanDisk SDIN7DP2-4G 4 GB iNAND Ultra Flash Memory
- Qualcomm Atheros QCA6234X-AM2D Wi-Fi and Bluetooth Module
- Texas Instruments TPS65910A1 Integrated Power Management IC
Echo Sensors \(^1\) - 7 microphones

- Texas Instruments LP55231 Programmable 9-Output LED Driver (x4)
- Texas Instruments TLV320ADC3101 92dB SNR Low-Power Stereo ADC (x4)
- Texas Instruments SN74LVC74A Dual Positive-Edge-Triggered D-Type Flip-Flops
- S1053 0090 V6 Microphone (x7)
Echo Findings

- Identify the location of the Echo
- Nmap Scan to identify any possible open ports
- Basic Denial of Service attack

```
root@kali:~# aireplay-ng --deauth 1000 -a 10:0E:7E:80:36:81 mon0
```

Denial of Service attack

```
root@kali:~# nmap -p -A 10.35.112.49
```

Nmap Scan

```plaintext
Starting Nmap 6.47 ( http://nmap.org ) at 2016-04-06 14:45 EDT
Stats: 0:00:39 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 11.50% done; ETC: 14:59 (0:03:05 remaining)
Nmap scan report for 10.35.112.49
Host is up.
All 1000 scanned ports on 10.35.112.49 are filtered
Too many fingerprints match this host to give specific OS details

TRACEROUTE (using proto 1/icmp)
HOP RTT ADDRESS
1 ... 30
```
Amazon Echo Packet Capture

Traffic in Standby mode

Clear Text-Traffic for voice commands
• The AP to which the Echo is connected to talks to several unknown IP’s.
Clear Text HTTP Traffic & Top Conversations
Conclusion – Amazon Echo

• Constantly probes all the access points within its reach.
• Voice requests being sent are visible in plain text.
• Device uses two different MAC addresses.
• Packets being transmitted are encrypted.
• An optimal target to breach a network.
Device 2 - Samsung Smart TV

Smart TV
Access your favorite program choices, live TV, video on demand, apps, and social media in one easy-to-browse navigation experience.

SMART INTERACTION
• Motion Control with Optional Camera Accessory
• Voice Control
• Any Net Technology that allows one remote to control all digital devices in a home theater/entertainment system.

Smart Remote Control
Take ultimate control of your Smart TV – use the touchpad to navigate quickly, perform voice commands with the built-in microphone, or use the remote like a mouse and simply point and click.
Verboseness

Constant Talker

Contact AD Platform
Voice Commands – Clear Text

GET /search?q=Go%20to%20google%20information%20security&aq=f&aql=g147&aql=&oq=&gs_tai=HTTP/1.1
Host: www.google.com

GET /client_204?&atyp=!&biw=1112&bih=542&ei=mcIUV7CQHqG6jgT6gJHIAw HTTP/1.1
Host: www.google.com
Referer: http://www.google.com/search?q=northstarsoccer.org&oq=northstarsoccer.org&gs_i=heirloom-serp.3...30275.55874.0.57449.21.11.1.9.2.0.122.951.9j2.11.0....0...1ac.1j4.34.heirloom-serp..8.13.954.92vHApufTvM

296 DNS Queries
Samsung Smart TV Findings

• Setup is quite easy
• Once connected to the Internet, conducted packet capture
• Vulnerable to De-authentication attack similar to the Echo.

Packets Captured
Conclusion – Samsung Smart TV

• Data is being transmitted in Clear Text.
• Sends a minimum and 296 DNS queries as soon as it starts, and increase exponentially while being used.
• Voice commands given are visible in clear text.
• Highly talkative and pings several third-parties.
• A optimal security target
• *Why would an organization have data sent to more than one location?*
Scenario 2: A Sandwich

- Ordered sandwich by number
- Paid cash
- Siri enabled
- Would you like fries with that?

...result?
BOGO Chicken Maple Sausage Muffin Sandwich

Our breakfast sandwiches are made fresh just for you. Juicy maple sausage, fluffy egg white, and melted cheese on a toasted English Muffin. For a limited time buy one and get another for free!

Offer valid at participating locations. Expires September 30, 2019

Please add a link to your email to your safe sender list or address book. For instructions, please go here.

About This Message:

Sonic Rewards values its members and respects their privacy. To manage the communications you get, please click here. If you wish to unsubscribe from email communications, you can follow the unsubscribe link at the bottom of each email. For more information about our privacy policy, please click on the following link: Privacy Policy. If you want to contact Sonic Rewards, please visit our site.

To request in writing:
Sonic Rewards LLC,
PO Box 722, Sioux City, IA 51102-0722.
Scenario 3: Ring Doorbell
Ring Doorbell

- Works with Alexa to illuminate and send announcements to Echo devices when your doorbell is pressed or motion is detected. You can also see, hear, and talk to visitors through Echo Show or Echo Spot.
- Lets you see, hear and speak to visitors from your phone, tablet and PC
- Sends alerts as soon as motion is detected or when visitors press the Doorbell
- Works on any home, with or without existing doorbell wires
- Monitors your home in HD video with infrared night vision
- Lets you check-in on your property at anytime with Live View on-demand video
- Includes Lifetime Theft Protection: If your Doorbell gets stolen, we’ll replace it for free
Ring Doorbell

• Works with Alexa to illuminate and send announcements to Echo devices when your doorbell is pressed or motion is detected. You can also see, hear, and talk to visitors through Echo Show or Echo Spot.

• Lets you see, hear and speak to visitors from your phone, tablet and PC

• Sends alerts as soon as motion is detected or when visitors press the Doorbell

• Works on any home, with or without existing doorbell wires

• Monitors your home in HD video with infrared night vision

• Lets you check-in on your property at anytime with Live View on-demand video

• Includes Lifetime Theft Protection: If your Doorbell gets stolen, we’ll replace it for free
Ring Doorbell Privacy Policy – Information we collect about you

• We obtain certain personal information in connection with the products and services we provide. The types of personal information we obtain include:
• Contact information, such as name, phone number, and email and postal address;
• Account information, such as online password and other log-in details used to access Ring products and services;
• Payment information, such as name, billing address and payment card details, including card number, expiration date and security code, which is collected and stored by our third-party payment processor on our behalf. Ring stores only the last four digits of your payment card and the expiration date;
• The geolocation of your mobile device if you consent to the collection of this data;
• Product setup information, such as the name and description of your Ring product (for example, “Ring Doorbell – Front Door”) and the location where you install your Ring product, and adjustments you make to the product setup;
Ring Doorbell Privacy Policy – Information we collect about you

- Technical information about your Ring product, such as your Wi-Fi network information and signal strength, and your Ring product’s model, serial number and software version;
- Social media handles, content and other data posted on our official social media pages;
- Information we obtain from third-party social media services (e.g., Facebook) or payment services (e.g., PayPal) if you choose to link to, create or log into your Ring account through these services (including when you share Ring videos or content via your social media account);
- Information we obtain from third-party business partners if you choose to use our Ring+ Service, such as your account ID, account name and email address;
- Information you submit in connection with a career opportunity at Ring, such as contact details, information in your resume and details about your current employment;
- Other personal information contained in content you submit to us, such as through our “Contact Us” feature or customer support tools on our websites or mobile apps.
Ring Doorbell Privacy Policy – How we use information we collect about you

• Provide our products and services to you;
• Establish and manage your Ring account and profile;
• Process and fulfill claims and orders in connection with our products and services and keep you informed about the status of your order;
• Personalize your experience with our products and services;
• Allow you to stream, save and share content through our services;
• Identify and authenticate you so you may access certain content or use certain of our services;
• Increase and maintain the safety and security of our products and services and prevent misuse;
Ring Doorbell Privacy Policy – How we use information we collect about you

- Perform analytics (including market and consumer research, trend analysis, financial analysis, and anonymization of personal information);
- Manage career opportunities at Ring; including for recruitment purposes, employee onboarding and other HR purposes;
- Operate, evaluate, develop, manage and improve our business (including operating, administering, analyzing and improving our products and services; developing new products and services; managing and evaluating the effectiveness of our communications; performing accounting, auditing, billing reconciliation and collection activities and other internal functions);
- Protect against, identify and prevent fraud and other criminal activity, claims and other liabilities; and
- Comply with and enforce applicable legal requirements, relevant industry standards and policies, including this Privacy Notice and our Terms of Service.
- We also may use the personal information we collect about you in other ways for which we provide specific notice at the time of collection and obtain your consent if required by applicable law.
List of Third-Party Analytics Services (Last updated May 22, 2018)

• We use the third-party data analytics platforms listed below to evaluate use of our website and mobile apps. To learn more about these analytics services’ information practices and how to opt-out, please visit their privacy policies and opt-out pages linked below.

• Google Analytics: Privacy Policy; opt-out
  Mixpanel: Privacy Policy; opt-out
  HotJar: Privacy Policy; opt-out
  Optimizely: Privacy Policy; opt-out
• We also may disclose personal information about you (1) if we are required to do so by law or legal process (such as a court order or subpoena); (2) in response to requests by government agencies, such as law enforcement authorities; (3) to establish, exercise or defend our legal rights; (4) when we believe disclosure is necessary or appropriate to prevent physical or other harm or financial loss; (5) in connection with an investigation of suspected or actual illegal activity; or (6) otherwise with your consent.

• We reserve the right to transfer any personal information we
• This Privacy Notice may be updated periodically and without prior notice to you to reflect changes in our personal information practices. We will post a notice on our websites and mobile apps to notify you of significant changes to our Privacy Notice and indicate at the top of the notice when it was most recently updated.
Ring Doorbell – Reality

• A new patent application envisions using a combination of doorbell cameras and facial recognition technology to build a system that could be used to match images of people who show up at your door to a “suspicious persons” database.
• a Ring R&D team in Ukraine could access a folder containing “every video created by every Ring camera around the world.” Additionally, as if that wasn’t bad enough, those employees could also access a “corresponding database that linked each specific video file to corresponding specific Ring customers.”

• The videos were also...unencrypted. Reason? Ring decided it was too expensive.
Scenario 4 - ∞

- Target – third party
- Equifax
- Capitol One – third party (AWS)
- Atlanta - Ransomware
- Baltimore - Ransomware
- 22 Texas municipalities - Ransomware – third party
Is there a Solution or at least a Compromise?

Validation
Incident response has grown into far more than forensic analysis of a workstation. With this growth has come many challenges and developments ranging from educating the digital forensic and cyber security workforce to addressing the many threats that advanced technology and Big Data present - not only from terrorists and cyber criminals, but also from the commercial sector.
Data collection sources, techniques and analytical processes: What's the Big Data deal?

- We have not learned basic lessons from history.
- The IoT adds considerable complexity for defense and incident response in addition to the legal and ethical issues including liability.
- Unlikely threat origination sources
- Scope creep is highly likely
- Don’t overlook mobile platforms
- Auditors have the opportunity to be the adults in the room
Resources – Environment

• Ferris State University Information Security & Intelligence Digital Forensic Research Lab w/ segmented network
• ABET Accredited in Cybersecurity
• Information Security & Intelligence program – est. 2007
• Ranked #1 in Michigan and top 25 Nationally
• First program to combine Cyber Security & Intelligence

• Link and Visual Analysis
• Competitive Theory
• Penetration Testing
• Risk Analysis
• Secure Technologies
• Project Management
• Fraud

• Information Security
• Digital Forensics
• Secure Database
• Python
• Data Mining
• Open Source Intelligence
• Legal/Ethical Issues
Resources – Tools

- Wireshark and Tshark
- Isolated WLAN and LAN
- Win7 and Kali Linux
- Network Miner Pro
- Network Tap
  - Dualcomm DCSW-1005PT 10/100 Ethernet Network TAP w/PoE
- Steelcentral Packet Analyzer
- Acrylic Wifi Analyzer
- Palo Alto PA200 Firewall
- AirPcap – WLAN Capture Cards
- Nexpose Vulnerability
References


Data collection sources, techniques and analytical processes: What's the Big Data deal?

Questions?

Greg Gogolin, Ph.D.
CISSP, EnCE, PMP